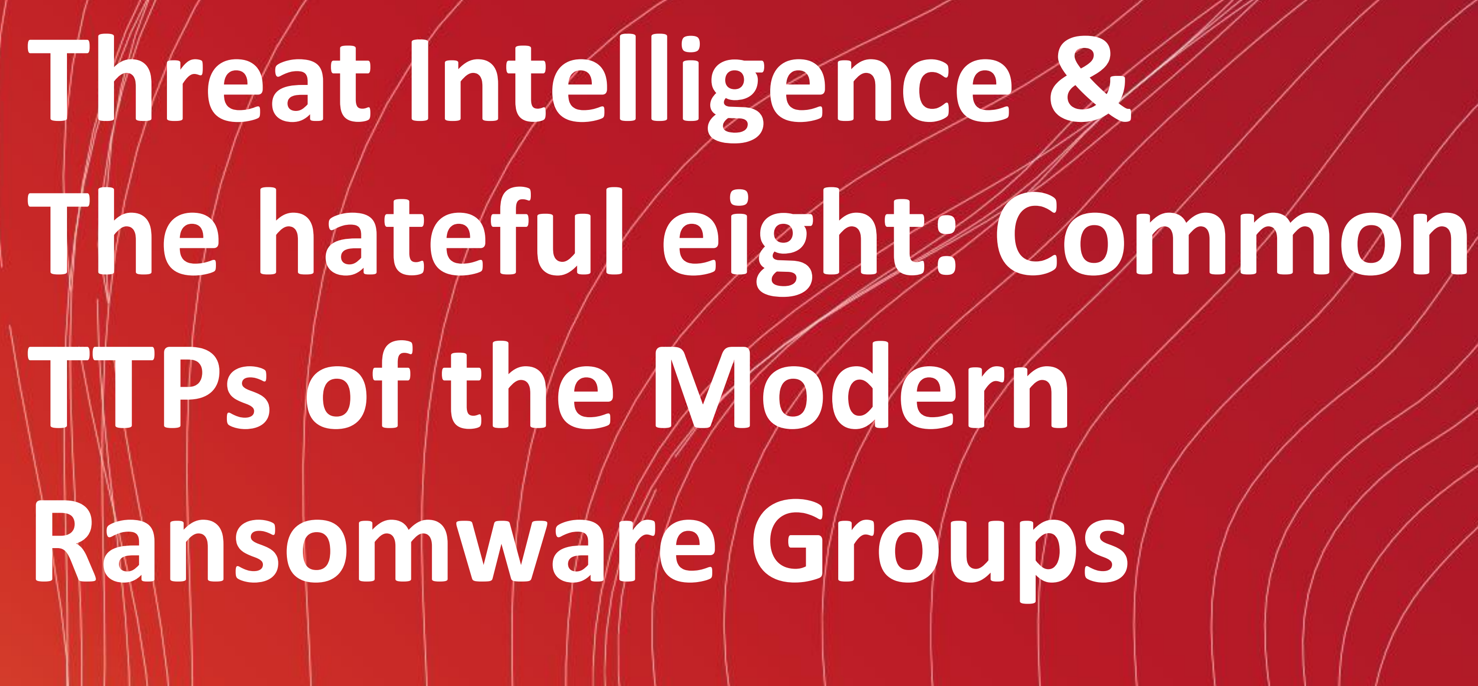


Threat Intelligence & The hateful eight: Common TTPs of the Modern Ransomware Groups

Nikita Nazarov,
Head of Threat Exploration



О чём будем говорить:

Первая часть:

- Cyber Kill Chain как начало точки отсчёта современного TI;
- F2T2EA - FIND FIX TRACK TARGET ENGAGE ASSESS;
- Intelligence-Driven Defense;
- Рождение MITRE ATT&CK®;
- Пирамида боли Дэвида Бианко;

Вторая часть:

- The hateful eight: Common TTPs of the Modern Ransomware Groups

“Если знаешь противника и знаешь себя, сражайся хоть сто раз, опасности не будет; если знаешь себя, а его не знаешь, один раз победишь, другой раз потерпишь поражение; если не знаешь ни себя, ни его, каждый раз, когда будешь сражаться, будешь терпеть поражение.”

Сунь-Цзы «Искусство войны»

Cyber Kill Chain

Intrusion Kill Chain

Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command and Control (C2)	Actions on Objectives
Research, identification and selection of targets, often represented as crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies	Coupling a remote access trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). Increasingly, client applications data files such as Adobe PDF or Microsoft Office documents serve as the weaponized deliverable	Transmission of the weapon to the targeted environment using vectors like email attachments, websites, and USB removable media.	After the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability.	Installation of a remote access trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.	Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel	Only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically this objective is data exfiltration which involves collecting, encrypting and extracting information from the victim environment.

Detect, → Deny → Disrupt → Degrade → Deceive → Destroy

Leverage, discover, analyze → Atomic, computed and behavior indicators

Campaign Analysis – Tools, Techniques and Procedures

- 1996 F2T2EA
- 2011 Cyber Kill Chain
- 2012 Intelligence - Driven Defense
- 2013 - ATT&CK Matrix

F2T2EA



Figure 1-1. F2T2EA

The Find, Fix, Track Target, Engage, Assess (F2T2EA) methodology seen in Figure 1-1 mechanizes the operational level "kill chain" during the execution process. Theater and national assets/resources detect objectives of potential significance (find). These systems identify and determine the location of a target (fix). From this location, tracking systems acquire and monitor the object (track). Dynamic decision-making then directs resources (target), and applies capabilities (engage) in a timely and decisive manner. To assure the desired effect, an assessment (assess) occurs during or after engagement to determine whether the target should be reattacked. These sequential steps describe a critical path that must occur for each dynamic event.

- 1996 F2T2EA
- 2011 Cyber Kill Chain
- 2012 Intelligence - Driven Defense
- 2013 - ATT&CK Matrix

TABLE I. KEY INDICATORS OF KILL CHAINS

Phase	Indicators
Find	detection range(km), transmit power(kW), endurance(h), working frequency(MHz), pulse width(μs), pulse repetition rate(kHz), antenna length(m), radome thickness(m), azimuth beam width(°), elevation beam width(°), antenna side lobe（dB）
Fix	transmit power(kW), received frequency(MHz), dynamic range(dB), sensitivity(dBv), output power(kW), MTBF(h), peak power(w), recognition range (km)
Track	target tracking capacity, angular accuracy(°), velocity measurement range（kn）, clutter improvement factor(dB), operating range(km), endurance(h), MTBF(h)
Target	navigation capability, target processing capacity, azimuth(°), data transfer rate(kbps), working frequency(MHz), operating range(km)
Engage	tactical range(km), service ceiling(m), maximum suspension weight(kg), maximum level flight speed(km/h), hitting probability(%),maximum attack range(km), maximum missile speed(km/h)
Assess	endurance(h), transmit frequency(MHz), received frequency(MHz), dynamic range(dB), sensitivity(dBv) , operating range(km) , MTBF(h)

Intelligence-Driven Defense

Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

Eric M. Hutchins[*], Michael J. Cloppert[†], Rohan M. Amin, Ph.D.[‡]

Lockheed Martin Corporation

Abstract

Conventional network defense tools such as intrusion detection systems and anti-virus focus on the vulnerability component of risk, and traditional incident response methodology presupposes a successful intrusion. An evolution in the goals and sophistication of computer network intrusions has rendered these approaches insufficient for certain actors. A new class of threats, appropriately dubbed the "Advanced Persistent Threat" (APT), represents well-resourced and trained adversaries that conduct multi-year intrusion campaigns targeting highly sensitive economic, proprietary, or national security information. These adversaries accomplish their goals using advanced tools and techniques designed to defeat most conventional computer network defense mechanisms. Network defense techniques which leverage knowledge about these adversaries can create an intelligence feedback loop, enabling defenders to establish a state of information superiority which decreases the adversary's likelihood of success with each subsequent intrusion attempt. Using a kill chain model to describe phases of intrusions, mapping adversary kill chain indicators to defender courses of action, identifying patterns that link individual intrusions into broader campaigns, and understanding the iterative nature of intelligence gathering form the basis of intelligence-driven computer network defense (CND). Institutionalization of this approach reduces the likelihood of adversary success, informs network defense investment and resource prioritization, and yields relevant metrics of performance and effectiveness. The evolution of advanced persistent threats necessitates an intelligence-based model because in this model the defenders mitigate not just vulnerability, but the threat component of risk, too.

1996 F2T2EA
2011 Cyber Kill Chain
2012 Intelligence - Driven Defense
2013 - ATT&CK Matrix

Intelligence-Driven Defense - Courses of Action

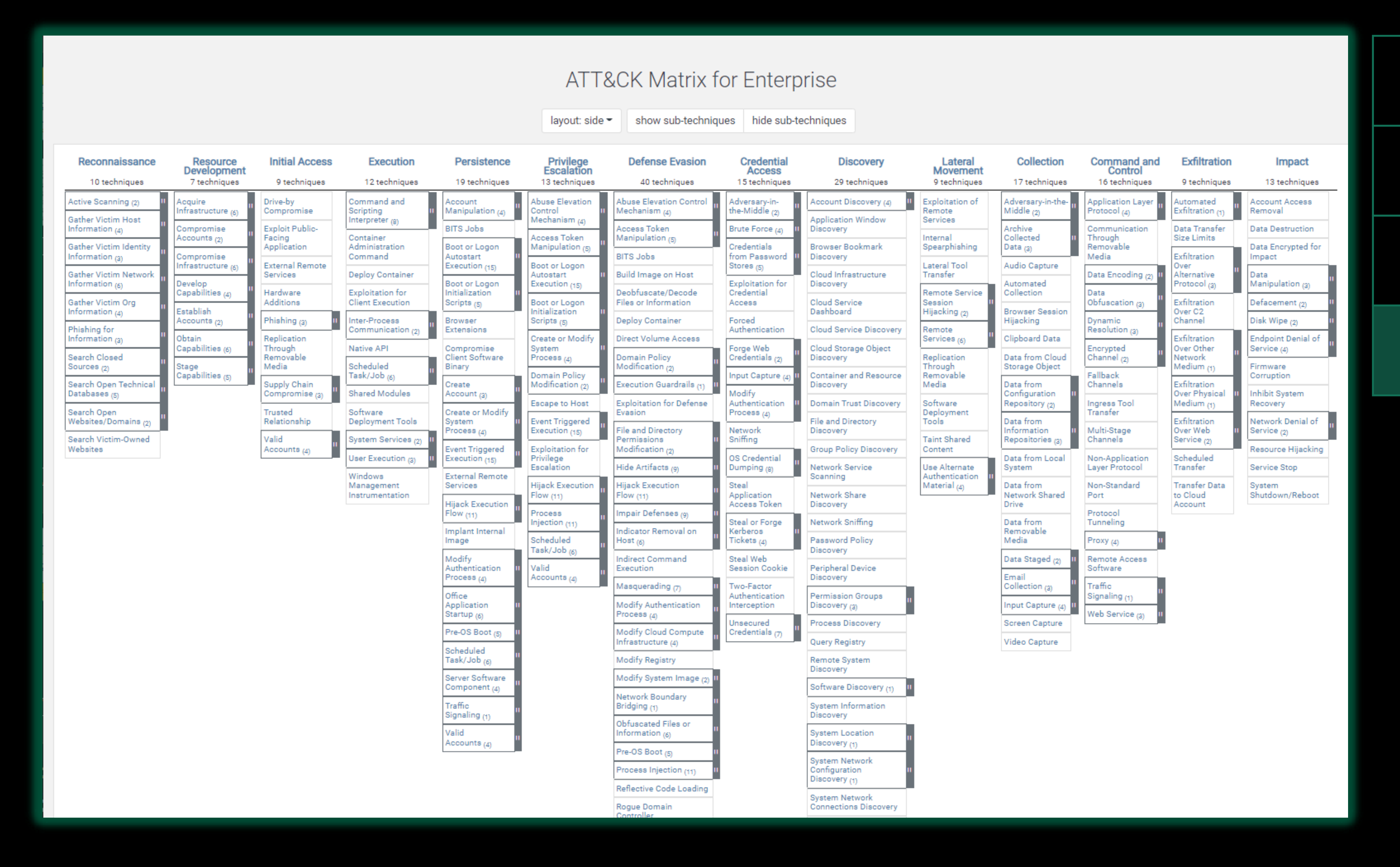
Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

- 1996 F2T2EA
- 2011 Cyber Kill Chain
- 2012 Intelligence - Driven Defense
- 2013 - ATT&CK Matrix

“ “Если хочешь идти быстро — иди один, если хочешь идти далеко — идите вместе.”

Африканская пословица

MITRE ATT&CK



1996 F2T2EA

2011 Cyber Kill Chain

2012 Intelligence - Driven Defense

2013 - ATT&CK Matrix

MITRE ATT&CK

Reconnaissance (10 techniques)
- Active Scanning (2): Scanning IP Blocks; Vulnerability Scanning
- Gather Victim Host Information (4): Hardware; Software; Firmware; Client Configurations
- Gather Victim Identity Information (3): Credentials; Email Addresses; Employee Names
- Gather Victim Network Information (6): Domain Properties; DNS; Network Trust Dependencies; Network Topology; IP Addresses; Network Security Appliances
- Gather Victim Org Information (4): Business Relationships; Determine Physical Locations; Identify Business Tempo; Identify Roles
- Phishing for Information (3): Spearphishing Service; Spearphishing Attachment; Spearphishing Link
- Search Closed Sources (2): Threat Intel Vendors; Purchase Technical Data
- Search Open Technical Databases (5): WHOIS; DNS/Passive DNS; Digital Certificates; CDNs; Scan Databases
- Search Open Websites/Domains (2): Social Media; Search Engines
- Search Victim-Owned Websites

Resource Development (7 techniques)
- Acquire Infrastructure (6): Domains; DNS Server; Virtual Private Server; Server; Botnet; Web Services
- Compromise Accounts (2): Social Media Accounts; Email Accounts
- Compromise Infrastructure (6): Domains; DNS Server; Virtual Private Server; Server; Botnet; Web Services
- Develop Capabilities (4): Malware; Code Signing Certificates; Digital Certificates; Exploits
- Establish Accounts (2): Social Media Accounts; Email Accounts
- Obtain Capabilities (6): Malware; Tool; Code Signing Certificates; Digital Certificates; Exploits; Vulnerabilities
- Stage Capabilities (5): Upload Malware; Upload Tool; Install Digital Certificate; Drive-by Target; Link Target

Initial Access (9 techniques)
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3): Spearphishing Attachment; Spearphishing Link; Spearphishing via Service
- Replication Through Removable Media
- Supply Chain Compromise (3): Compromise Software Dependencies and Development Tools; Compromise Software Supply Chain; Compromise Hardware Supply Chain
- Trusted Relationship
- Valid Accounts (4): Default Accounts; Domain Accounts; Local Accounts; Cloud Accounts

Execution (12 techniques)
- Command and Scripting Interpreter (8): PowerShell; AppleScript; Windows Command Shell; Unix Shell; Visual Basic; Python; JavaScript; Network Device CLI
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (2): Component Object Model; Dynamic Data Exchange
- Native API
- Scheduled Task/Job (6): At (Windows); Scheduled Task; At (Linux); Cron; Systemd Timers; Container Orchestration Job
- Shared Modules
- Software Deployment Tools
- System Services (2): Launchctl; Service Execution
- User Execution (3): Malicious Link; Malicious File; Malicious Image
- Windows Management Instrumentation

Persistence (19 techniques)
- Account Manipulation (4): Additional Cloud Credentials; Exchange Email Delegate Permissions; Add Office 365 Global Administrator Role; SSH Authorized Keys
- BITS Jobs
- Boot or Logon Autostart Execution (15): Registry Run Keys / Startup Folder; Authentication Package; Time Providers; Winlogon Helper DLL; Security Support Provider; Kernel Modules and Extensions; Re-opened Applications; LSASS Driver; Shortcut Modification; Port Monitors; Plist Modification; Print Processors; XDG Autostart Entries; Active Setup; Login Items
- Boot or Logon Initialization Scripts (5): Logon Script (Windows); Logon Script (Mac); Network Logon Script; RC Scripts; Startup Items
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3): Local Account; Domain Account; Cloud Account
- Create or Modify System Process (4): Launch Agent; Systemd Service; Windows Service; Launch Daemon
- Event Triggered Execution (15): Change Default File Association; Screensaver; Windows Management Instrumentation Event Subscription; Unix Shell Configuration Modification; Trap; LC_LOAD_DYLIB Addition; Netsh Helper DLL; Accessibility Features; AppCert DLLs; AppInit DLLs

Privilege Escalation (13 techniques)
- Abuse Elevation Control Mechanism (4): Setuid and Setgid; Bypass User Account Control; Sudo and Sudo Caching; Elevated Execution with Prompt
- Access Token Manipulation (5): Token Impersonation/Theft; Create Process with Token; Make and Impersonate Token; Parent PID Spoofing; SID-History Injection
- Boot or Logon Autostart Execution (15): Registry Run Keys / Startup Folder; Authentication Package; Time Providers; Winlogon Helper DLL; Security Support Provider; Kernel Modules and Extensions; Re-opened Applications; LSASS Driver; Shortcut Modification; Port Monitors; Plist Modification; Print Processors; XDG Autostart Entries; Active Setup; Login Items
- Boot or Logon Initialization Scripts (5): Logon Script (Windows); Logon Script (Mac); Network Logon Script; RC Scripts; Startup Items
- Create or Modify System Process (4): Launch Agent; Systemd Service; Windows Service; Launch Daemon
- Domain Policy Modification (2): Group Policy Modification; Domain Trust Modification
- Escape to Host
- Event Triggered Execution (15): Change Default File Association; Screensaver; Windows Management Instrumentation Event Subscription; Unix Shell Configuration Modification; Trap; LC_LOAD_DYLIB Addition; Netsh Helper DLL; Accessibility Features; AppCert DLLs; AppInit DLLs

Defense Evasion (40 techniques)
- Abuse Elevation Control Mechanism (4): Setuid and Setgid; Bypass User Account Control; Sudo and Sudo Caching; Elevated Execution with Prompt
- Access Token Manipulation (5): Token Impersonation/Theft; Create Process with Token; Make and Impersonate Token; Parent PID Spoofing; SID-History Injection
- BITS Jobs
- Build Image on Host
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (2): Group Policy Modification; Domain Trust Modification
- Execution Guardrails (1): Environmental Keying
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2): Windows File and Directory Permissions Modification; Linux and Mac File and Directory Permissions Modification
- Hide Artifacts (9): Hidden Files and Directories; Hidden Users; Hidden Window; NTFS File Attributes; Hidden File System; Run Virtual Instance; VBA Stomping; Email Hiding Rules; Resource Forking
- Hijack Execution Flow (11): Services File Permissions Weakness; Executable Installer File Permissions Weakness; Services Registry Permissions Weakness; Path Interception by Unquoted Path; Path Interception by PATH Environment Variable; Path Interception by Search Order Hijacking; DLL Search Order Hijacking; DLL Side-Loading; Dynamic Linker Hijacking; Dylib Hijacking; COR_PROFILER
- Disable or Modify Tools; Disable Windows Event Logging; Impair Command History Logging; Disable or Modify System Firewall

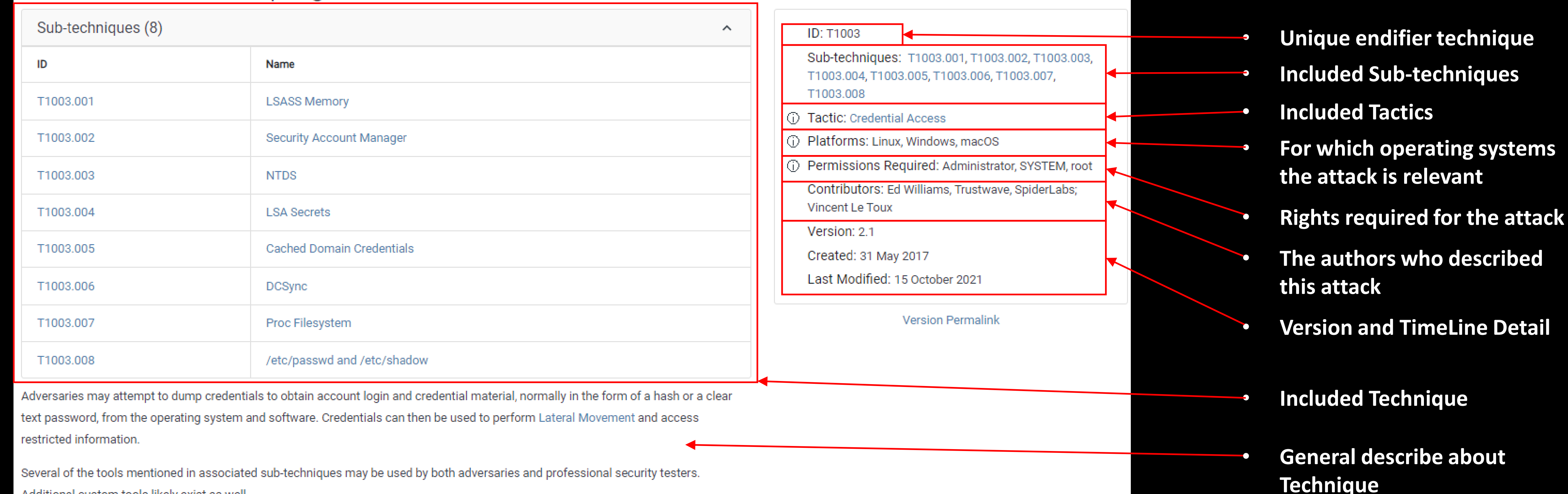
Credential Access (15 techniques)
- Adversary-in-the-Middle (2): LLMNR/NBT-NS Poisoning and SMB Relay; ARP Cache Poisoning
- Brute Force (4): Password Guessing; Password Cracking; Password Spraying; Credential Stuffing
- Credentials from Password Stores (5): Keychain; Securityd Memory; Credentials from Web Browsers; Windows Credential Manager; Password Managers
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2): Web Cookies; SAML Tokens
- Input Capture (4): Keylogging; GUI Input Capture; Web Portal Capture; Credential API Hooking
- Modify Authentication Process (4): Domain Controller Authentication; Password Filter DLL; Pluggable Authentication Modules; Network Device Authentication
- Network Sniffing
- OS Credential Dumping (8): LSASS Memory; Security Account Manager; NTDS; DCSync; Proc Filesystem; /etc/passwd and /etc/shadow; Cached Domain Credentials; LSA Secrets
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (4)

Discovery (29 techniques)
- Account Discovery (4): Local Account; Domain Account; Email Account; Cloud Account
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery: Domain Groups

Lateral Movement (9 techniques)
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2): SSH Hijacking; RDP Hijacking
- Remote Services (6): Remote Desktop Protocol; SMB/Windows Admin Shares; Distributed Component Object Model; SSH; VNC; Windows Remote Management
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (4): Pass the Hash; Pass the Ticket; Application Access Token; Web Session Cookie

Collection (17 techniques)
- Adversary-in-the-Middle (2): LLMNR/NBT-NS Poisoning and SMB Relay; ARP Cache Poisoning
- Archive Collected Data (3): Archive via Utility; Archive via Library; Archive via Custom Method
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (2): SNMP (MIB Dump); Network Device Configuration Dump
- Data from Information Repositories (3): Confluence; Sharepoint; Code Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2): Local Data Staging; Remote Data Staging
- Email Collection (3): Local Email Collection; Remote Email Collection; Email Forwarding Rule
- Input Capture (4): Keylogging; GUI Input Capture; Web Portal Capture; Credential API Hooking
- Screen Capture
- Video Capture

MITRE ATT&CK



- **Unique endifier technique**
- **Included Sub-techniques**
- **Included Tactics**
- **For which operating systems the attack is relevant**
- **Rights required for the attack**
- **The authors who described this attack**
- **Version and TimeLine Detail**
- **Included Technique**
- **General describe about Technique**

MITRE ATT&CK

Procedure Examples

ID	Name	Description
G0006	APT1	APT1 has been known to use credential dumping using Mimikatz.[5]
G0007	APT28	APT28 regularly deploys both publicly available (ex: Mimikatz) and custom password retrieval tools on victims.[6][7] They have also dumped the LSASS process memory using the MiniDump function.[8]
G0022	APT3	APT3 has used a tool to dump credentials by injecting itself into lsass.exe and triggering with the argument "dig."[9]
G0050	APT32	APT32 used Mimikatz and customized versions of Windows Credential Dumper to harvest credentials.[10][11]
G0064	APT33	APT33 has used a variety of publicly available tools like LaZagne, Mimikatz, and ProcDump to dump credentials.[12][13]
G0087	APT39	APT39 has used Mimikatz, Windows Credential Editor and ProcDump to dump credentials.[14]

- **Procedure Examples describes some cases relates with this Technique:**

  - Who used this Technique
  - Some Details
  - Links for sources

Mitigations

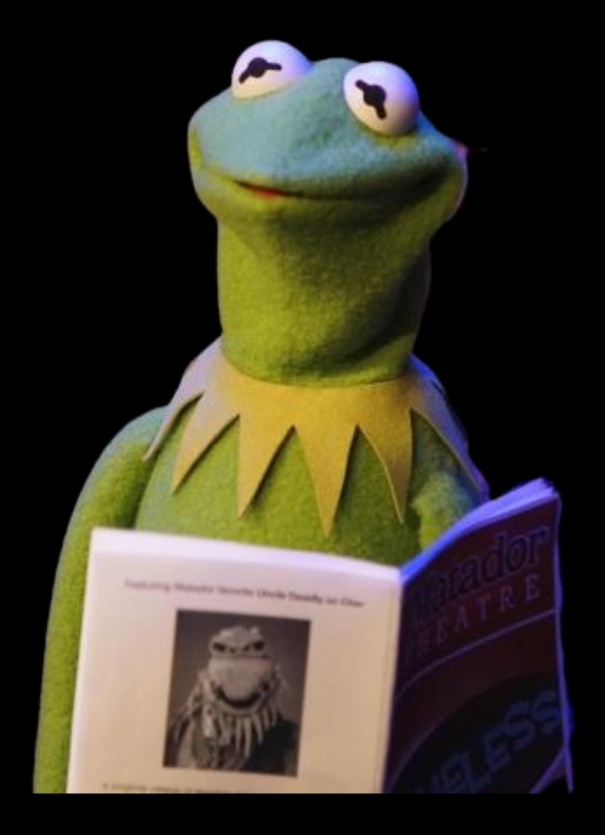
ID	Mitigation	Description
M1040	Behavior Prevention on Endpoint	On Windows 10, enable Attack Surface Reduction (ASR) rules to secure LSASS and prevent credential stealing. [74]
M1043	Credential Access Protection	With Windows 10, Microsoft implemented new protections called Credential Guard to protect the LSA secrets that can be used to obtain credentials through forms of credential dumping. It is not configured by default and has hardware and firmware system requirements. It also does not protect against all forms of credential dumping. [75][76]
M1028	Operating System Configuration	Consider disabling or restricting NTLM.[77] Consider disabling WDigest authentication.[78]
M1027	Password Policies	Ensure that local administrator accounts have complex, unique passwords across all systems on the network.
M1026	Privileged Account Management	Do not put user or admin domain accounts in the local administrator groups across systems unless they are tightly controlled, as this is often equivalent to having a local administrator account with the same password on all systems. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers.

- **Mitigations describes general advisees about how you can protect you environment**

MITRE ATT&CK

References

1. Gruzweig, J. et al. (2021, March 2). Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities. Retrieved March 3, 2021.
2. Symantec. (2021, June 10). Attacks Against the Government Sector. Retrieved September 28, 2021.
3. Graeber, M. (2014, October). Analysis of Malicious Security Support Provider DLLs. Retrieved March 1, 2017.
4. Wilson, B. (2016, April 18). The Importance of KB2871997 and KB2928120 for Credential Protection. Retrieved April 11, 2018.
5. Mandiant. (n.d.). APT1 Exposing One of China's Cyber Espionage Units. Retrieved July 18, 2016.
6. ESET. (2016, October). En Route with Sednit - Part 2: Observing the Comings and Goings. Retrieved November 21, 2016.
7. Mueller, R. (2018, July 13). Indictment - United States of America vs. VIKTOR BORISOVICH NETYKSHO, et al. Retrieved September 13, 2018.
8. NSA, CISA, FBI, NCSC. (2021, July). Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments. Retrieved July 26, 2021.
9. Symantec Security Response. (2016, September 6). Buckeye cyberespionage group shifts gaze from US to Hong Kong. Retrieved September 26, 2016.
10. Dahan, A. (2017, May 24). OPERATION COBALT KITTY: A LARGE-SCALE APT IN ASIA CARRIED OUT BY THE OCEANLOTUS GROUP. Retrieved November 5, 2018.
11. Dahan, A. (2017). Operation Cobalt Kitty. Retrieved December 27, 2018.
12. Security Response attack Investigation Team. (2019, March 27). Elfin: Relentless Espionage Group Targets Multiple Organizations in Saudi Arabia and U.S.. Retrieved April 10, 2019.
13. Ackerman, G., et al. (2018, December 21). OVERRULED: Containing a Potentially Destructive Adversary. Retrieved January 17, 2019.
14. Hawley et al. (2019, January 29). APT39: An Iranian Cyber Espionage Group Focused on Personal Information. Retrieved February 19, 2019.
15. Fraser, N., et al. (2019, August 7). Double DragonAPT41, a dual espionage and cyber crime operation APT41. Retrieved September 23, 2019.
16. Rostovcev, N. (2021, June 10). Big airline heist APT41 likely behind a third-party attack on Air India. Retrieved August 26, 2021.
17. M.Léveille, M-E.. (2017, October 24). Bad Rabbit: Not-Petya is back with improved ransomware. Retrieved January 28, 2021.
18. Lambert, T. (2020, May 7). Introducing Blue Mockingbird. Retrieved May 26, 2020.
19. Counter Threat Unit Research Team. (2017, October 12). BRONZE BUTLER Targets Japanese Enterprises. Retrieved January 4, 2018.
20. Cylance. (2014, December). Operation Cleaver. Retrieved September 14, 2017.
21. Strategic Cyber LLC. (2020, November 5). Cobalt Strike: Advanced Threat Tactics for Penetration Testers. Retrieved April 13, 2021.
22. F-Secure Labs. (2015, April 22). CozyDuke: Malware Analysis. Retrieved December 10, 2015.
23. DiMaggio, J. (2016, April 28). Tick cyberespionage group zeros in on Japan. Retrieved July 16, 2018.
24. Trend Micro. (2019, January 16). Exploring Emotet's Activities . Retrieved March 25, 2019.
25. Schroeder, W., Warner, J., Nelson, M. (n.d.). Github PowerShellEmpire. Retrieved April 28, 2016.
26. FireEye Threat Intelligence. (2016, April). Follow the Money: Dissecting the Operations of the Cyber Crime Group FIN6. Retrieved June 1, 2016.
27. McKeague, B. et al. (2019, April 5). Pick-Six: Intercepting a FIN6 Intrusion, an Actor Recently Tied to Ryuk and LockerGoga Ransomware. Retrieved April 17, 2019.
28. Elovitz, S. & Ahl, I. (2016, August 18). Know Your Enemy: New Financially-Motivated & Spear-Phishing Group. Retrieved February 26, 2018.
42. Plan, F., et al. (2019, March 4). APT40: Examining a China-Nexus Espionage Actor. Retrieved March 18, 2019.
43. Mandiant. (2018). Mandiant M-Trends 2018. Retrieved July 9, 2018.
44. Deply, B. (n.d.). Mimikatz. Retrieved September 29, 2015.
45. Deply, B., Le Toux, V. (2016, June 5). module ~ lsadump. Retrieved August 7, 2017.
46. Grafnetter, M. (2015, October 26). Retrieving DPAPI Backup Keys from Active Directory. Retrieved December 19, 2017.
47. The Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), the New Zealand National Cyber Security Centre (NZ NCSC), CERT New Zealand, the UK National Cyber Security Centre (UK NCSC) and the US National Cybersecurity and Communications Integration Center (NCCIC). (2018, October 11). Joint report on publicly available hacking tools. Retrieved March 11, 2019.
48. Lancaster, T.. (2017, November 14). Muddying the Water: Targeted Attacks in the Middle East. Retrieved March 15, 2018.
49. Symantec DeepSight Adversary Intelligence Team. (2018, December 10). Seedworm: Group Compromises Government Agencies, Oil & Gas, NGOs, Telecoms, and IT Firms. Retrieved December 14, 2018.
50. Peretz, A. and Theck, E. (2021, March 5). Earth Vetala – MuddyWater Continues to Target Organizations in the Middle East. Retrieved March 18, 2021.
51. Chiu, A. (2016, June 27). New Ransomware Variant "Nyetya" Compromises Systems Worldwide. Retrieved March 26, 2019.
52. US-CERT. (2017, July 1). Alert (TA17-181A): Petya Ransomware. Retrieved March 15, 2019.
53. Unit 42. (2017, December 15). Unit 42 Playbook Viewer. Retrieved December 20, 2017.
54. Davis, S. and Caban, D. (2017, December 19). APT34 - New Targeted Attack in the Middle East. Retrieved December 20, 2017.
55. Bromiley, M., et al.. (2019, July 18). Hard Pass: Declining APT34's Invite to Join Their Professional Network. Retrieved August 26, 2019.
56. Hromcova, Z. (2019, July). OKRUM AND KETRICAN: AN OVERVIEW OF RECENT KE3CHANG GROUP ACTIVITY. Retrieved May 6, 2020.
57. Mercer, W. and Rascagneres, P. (2018, February 12). Olympic Destroyer Takes Aim At Winter Olympics. Retrieved March 14, 2019.
58. Dantzig, M. v., Schamper, E. (2019, December 19). Operation Wocao: Shining a light on one of China's hidden hacking groups. Retrieved October 8, 2020.
59. Windows Defender Advanced Threat Hunting Team. (2016, April 29). PLATINUM: Targeted attacks in South and Southeast Asia. Retrieved February 15, 2018.
60. Mercer, W, et al. (2020, April 16). PoetRAT: Python RAT uses COVID-19 lures to target Azerbaijan public and private sectors. Retrieved April 27, 2020.
61. Nettitude. (2018, July 23). Python Server for PoshC2. Retrieved April 23, 2019.
62. PowerShellMafia. (2012, May 26). PowerSploit - A PowerShell Post-Exploitation Framework. Retrieved February 6, 2018.
63. PowerSploit. (n.d.). PowerSploit. Retrieved February 6, 2018.
64. Nicolas Verdier. (n.d.). Retrieved January 29, 2018.
65. CERT-FR. (2020, April 1). ATTACKS INVOLVING THE MESPINOZA/PYSA RANSOMWARE. Retrieved March 1, 2021.
66. Cherepanov, A.. (2016, December 13). The rise of TeleBots: Analyzing disruptive KillDisk attacks. Retrieved June 10, 2020.
67. Cherepanov, A.. (2017, June 30). TeleBots are back: Supply chain attacks against Ukraine. Retrieved June 11, 2020.
68. Group-IB. (2018, September). Silence: Moving Into the Darkside. Retrieved May 5, 2020.



MITRE ATT&CK


Initial Access
9 techniques
Execution
12 techniques
Persistence
19 techniques
Privilege Escalation
13 techniques
Defense Evasion
40 techniques
Credential Access
15 techniques
Discovery
29 techniques
Lateral Movement
9 techniques
Collection
17 techniques
Tactic Row Background
Scoring Gradient
Low value:
High value:
add another color
presets
and and Control
16 techniques
Exfiltratio
9 technique

MITRE ATT&CK

- **Who are we ?**
- **What APTs are attacking our sphere?**
- **What adversary's are dangerous for us?**
- **What does our environment consist of?**
- **What are our most valuable assets ?**
- **What protections do we have ?**
- **…**
- **…**
- **…**



MITRE ATT&CK

Home > Groups > APT39

APT39

APT39 is one of several names for cyberespionage activity conducted by the Iranian Ministry of Intelligence and Security (MOIS) through the front company Rana Intelligence Computing since at least 2014. APT39 has primarily targeted the travel, hospitality, academic, and telecommunications industries in Iran and across Asia, Africa, Europe, and North America to track individuals and entities considered to be a threat by the MOIS.[1][2][3][4][5]

ID: G0087
Associated Groups: REMIX KITTEN, ITG07, Chafer
Version: 3.1
Created: 19 February 2019
Last Modified: 12 October 2021

Version Permalink

- General describe about actor and it activity in the world

Associated Group Descriptions

Name	Description
REMIX KITTEN	[6]
ITG07	[3][4][5]
Chafer	Activities associated with APT39 largely align with a group publicly referred to as Chafer.[1][2][7][3][4][5]

- Related alias

Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	APT39 has used HTTP in communications with C2.[8][3]
		.004	Application Layer Protocol: DNS	APT39 has used remote access tools that leverage DNS in communications with C2.[8]
Enterprise	T1560	.001	Archive Collected Data: Archive via Utility	APT39 has used WinRAR and 7-Zip to compress an archive stolen data.[1]
Enterprise	T1197		BITS Jobs	APT39 has used the BITS protocol to exfiltrate stolen data from a compromised host.[3]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	APT39 has maintained persistence using the startup folder.[1]
		.009	Boot or Logon Autostart Execution: Shortcut Modification	APT39 has modified LNK shortcuts.[1]

- Which TTPs they used in detected activity

The Pyramid of Pain

TTPs — Tough!

TOOLS — Challenging

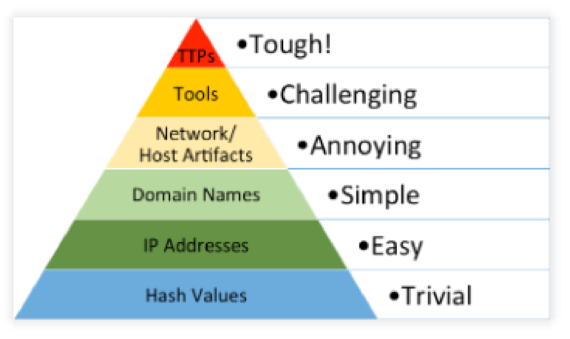
NETWORK/HOST ARTIFACTS — Annoying

DOMAIN NAMES — Simple

IP ADDRESSES — Easy

HASH VALUES — Trivial

The Pyramid of Pain



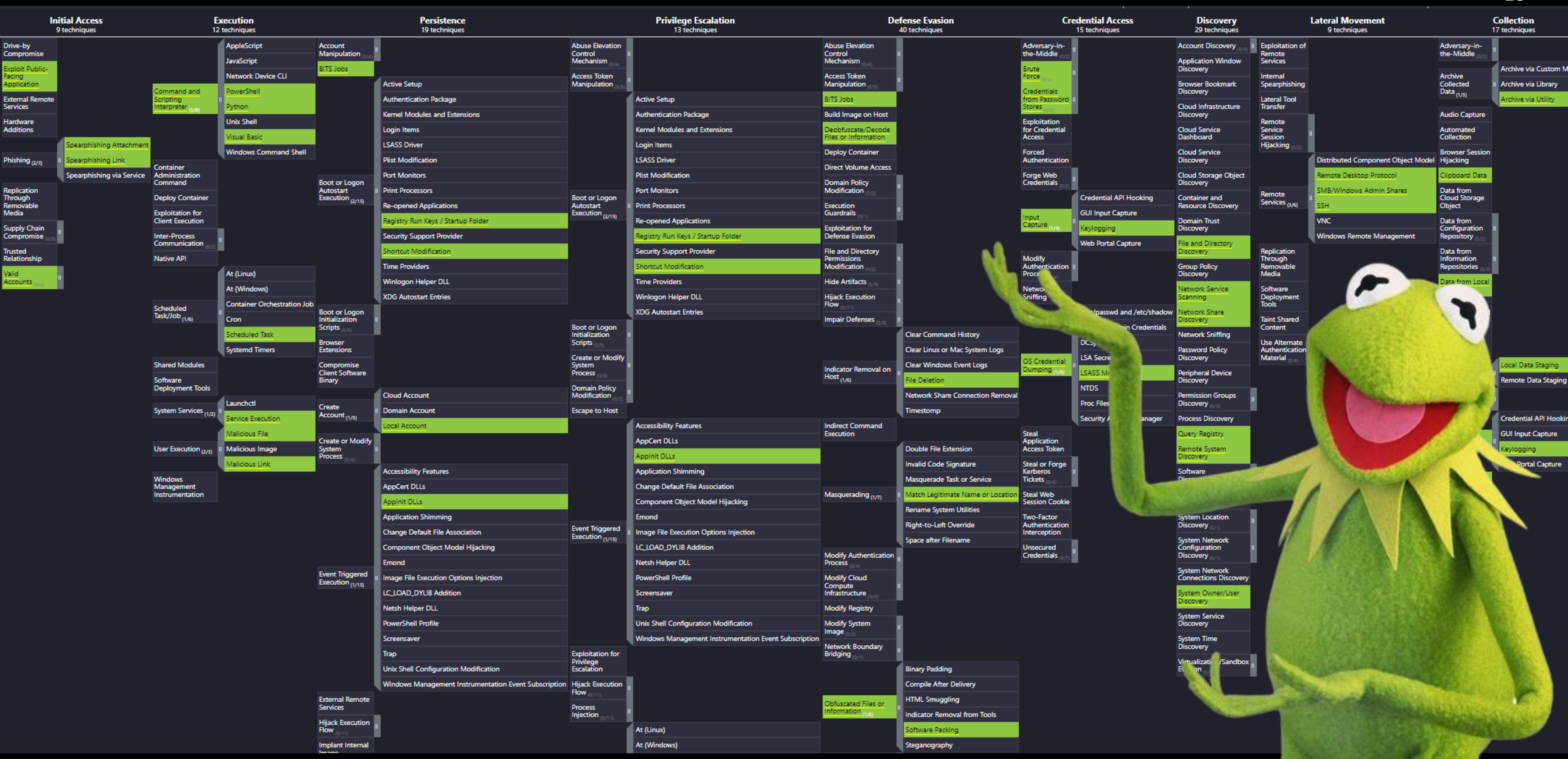
To illustrate this concept, I have created what I like to call the Pyramid of Pain. This simple diagram shows the relationship between the types of indicators you might use to detect an adversary's activities and how much pain it will cause them when you are able to deny those indicators to them. Let's examine this diagram in more detail.

Types of Indicators

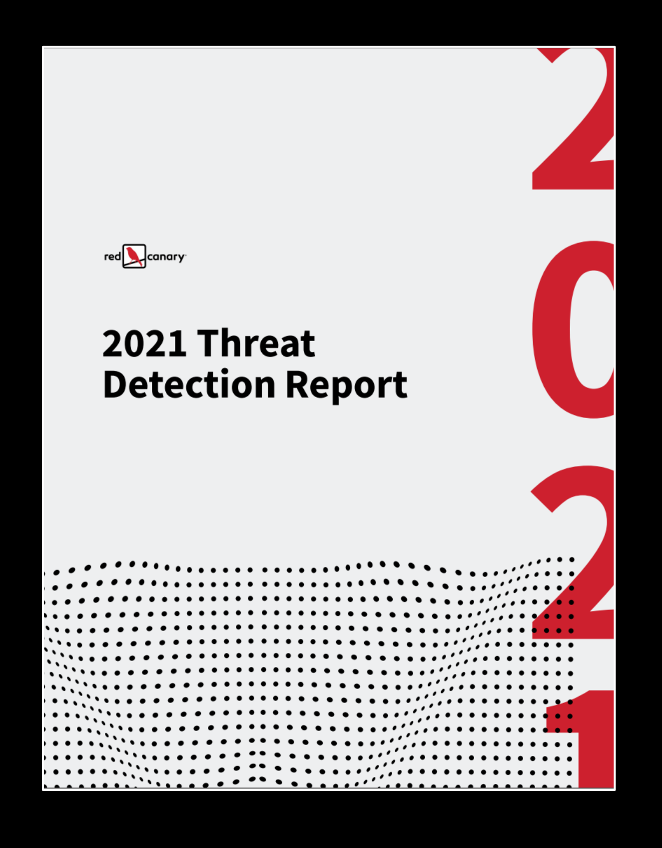
Let's start by simply defining types of indicators make up the pyramid:

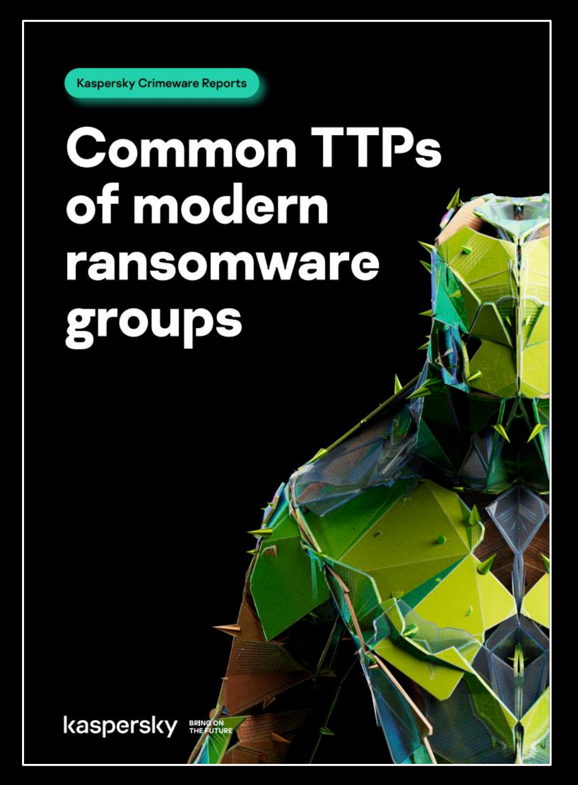
1. **Hash Values:** SHA1, MD5 or other similar hashes that correspond to specific suspicious or malicious files. Often used to provide unique references to specific samples of malware or to files involved in an intrusion.
2. **IP Addresses**: It's, um, an IP address. Or maybe a netblock.
3. **Domain Names**: This could be either a domain name itself (e.g., "evil.net") or maybe even a sub- or sub-sub-domain (e.g., "this.is.sooooo.evil.net")
4. **Network Artifacts**: Observables caused by adversary activities on your network. Technically speaking, every byte that flows over your network as a result of the adversary's interaction could be an artifact, but in practice this really means those pieces of the activity that might tend to distinguish malicious activity from that of legitimate users. Typical examples might be URI patterns, C2 information embedded in network protocols, distinctive HTTP User-Agent or SMTP Mailer values, etc.
5. **Host Artifacts**: Observables caused by adversary activities on one or more of your hosts. Again, we focus on things that would tend to distinguish malicious activities from legitimate ones. They could be registry keys or values known to be created by specific pieces of malware, files or directories dropped in certain places or using certain names, names or descriptions or malicious services or almost anything else that's distinctive.
6. **Tools**: Software used by the adversary to accomplish their mission. Mostly this will be things they bring with them, rather than software or commands that may already be installed on the computer. This would include utilities designed to create malicious documents for spearphishing, backdoors used to establish C2 or password crackers or other host-based utilities they may want to use post-compromise.
7. **Tactics, Techniques and Procedures (TTPs)**: How the adversary goes about accomplishing their mission, from reconnaissance all the way through data exfiltration and at every step in between. "Spearphishing" is a common TTP for establishing a presence in the network. "Spearphishing with a trojaned PDF file" or "... with a link to a malicious .SCR file disguised as a ZIP" would be more specific versions. "Dumping cached authentication credentials and reusing them in Pass-the-Hash attacks" would be a TTP. Notice we're not talking about specific tools here, as there are any number of ways of weaponizing a PDF or implementing Pass-the-Hash.

MITRE ATT&CK


Initial Access
9 techniques
Execution
12 techniques
Persistence
19 techniques
Privilege Escalation
13 techniques
Defense Evasion
40 techniques
Credential Access
15 techniques
Discovery
29 techniques
Lateral Movement
9 techniques
Collection
17 techniques
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (2/3)
Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Replication Through Removable Media
Supply Chain Compromise
Trusted Relationship
Valid Accounts
Command and Scripting Interpreter (7/8)
AppleScript
JavaScript
Network Device CLI
PowerShell
Python
Unix Shell
Visual Basic
Windows Command Shell
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication
Native API
Scheduled Task/Job (1/6)
At (Linux)
At (Windows)
Container Orchestration Job
Cron
Scheduled Task
Systemd Timers
Shared Modules
Software Deployment Tools
System Services (1/2)
Launchctl
Service Execution
User Execution (2/3)
Malicious File
Malicious Image
Malicious Link
Windows Management Instrumentation
Account Manipulation
BITS Jobs
Boot or Logon Autostart Execution (2/15)
Active Setup
Authentication Package
Kernel Modules and Extensions
Login Items
LSASS Driver
Plist Modification
Port Monitors
Print Processors
Re-opened Applications
Registry Run Keys / Startup Folder
Security Support Provider
Shortcut Modification
Time Providers
Winlogon Helper DLL
XDG Autostart Entries
Boot or Logon Initialization Scripts
Browser Extensions
Compromise Client Software Binary
Create Account (1/3)
Cloud Account
Domain Account
Local Account
Create or Modify System Process
Event Triggered Execution (1/15)
Accessibility Features
AppCert DLLs
AppInit DLLs
Application Shimming
Change Default File Association
Component Object Model Hijacking
Emond
Image File Execution Options Injection
LC_LOAD_DYLIB Addition
Netsh Helper DLL
PowerShell Profile
Screensaver
Trap
Unix Shell Configuration Modification
Windows Management Instrumentation Event Subscription
External Remote Services
Hijack Execution Flow
Implant Internal Image
Abuse Elevation Control Mechanism
Access Token Manipulation
Boot or Logon Autostart Execution (2/15)
Boot or Logon Initialization Scripts
Create or Modify System Process
Domain Policy Modification
Escape to Host
Event Triggered Execution (1/15)
Exploitation for Privilege Escalation
Hijack Execution Flow
Process Injection
At (Linux)
At (Windows)
BITS Jobs
Build Image on Host
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain Policy Modification
Execution Guardrails
Exploitation for Defense Evasion
File and Directory Permissions Modification
Hide Artifacts
Hijack Execution Flow
Impair Defenses
Indicator Removal on Host (1/6)
Clear Command History
Clear Linux or Mac System Logs
Clear Windows Event Logs
File Deletion
Network Share Connection Removal
Timestomp
Indirect Command Execution
Masquerading (1/7)
Double File Extension
Invalid Code Signature
Masquerade Task or Service
Match Legitimate Name or Location
Rename System Utilities
Right-to-Left Override
Space after Filename
Modify Authentication Process
Modify Cloud Compute Infrastructure
Modify Registry
Modify System Image
Network Boundary Bridging
Obfuscated Files or Information (1/6)
Binary Padding
Compile After Delivery
HTML Smuggling
Indicator Removal from Tools
Software Packing
Steganography
Adversary-in-the-Middle
Brute Force
Credentials from Password Stores
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials
Input Capture (1/4)
Credential API Hooking
GUI Input Capture
Keylogging
Web Portal Capture
Modify Authentication Process
Network Sniffing
OS Credential Dumping (1/8)
NTDS
Steal Application Access Token
Steal or Forge Kerberos Tickets
Steal Web Session Cookie
Two-Factor Authentication Interception
Unsecured Credentials
Account Discovery
Application Window Discovery
Browser Bookmark Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Network Service Scanning
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery
Process Discovery
Query Registry
Remote System Discovery
Software
System Location Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking
Remote Services (4/6)
Distributed Component Object Model
Remote Desktop Protocol
SMB/Windows Admin Shares
SSH
VNC
Windows Remote Management
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material
Adversary-in-the-Middle
Archive Collected Data (1/3)
Archive via Library
Archive via Utility
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage Object
Data from Configuration Repository
Data from Information Repositories
Local Data Staging
Remote Data Staging
Credential API Hooking
GUI Input Capture
Keylogging

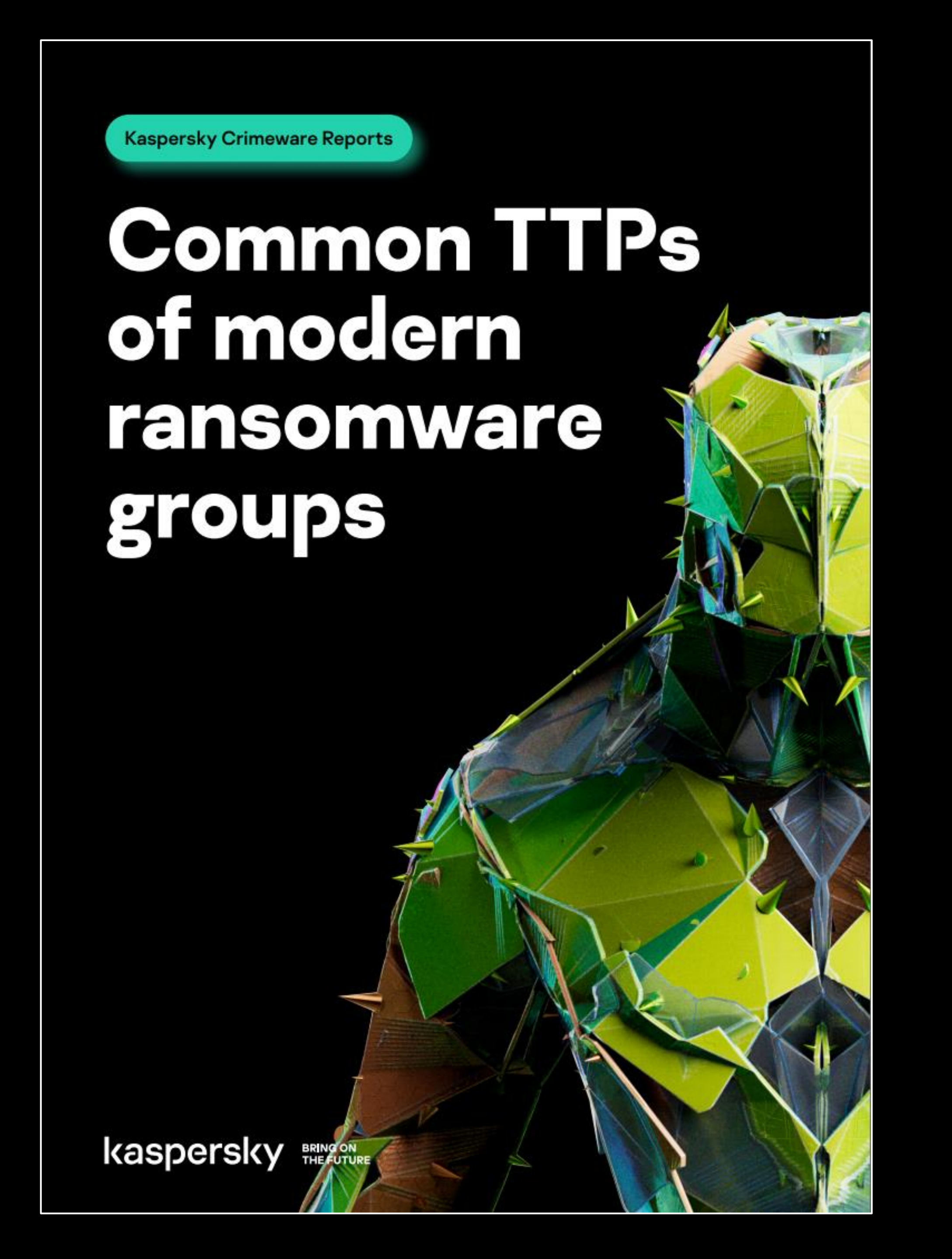
Other Sources for Global Threat Analysis










Kaspersky Crimeware Reports
Common TTPs of modern ransomware groups
kaspersky
BRING ON THE FUTURE

“Intelligence – is the glue that can bind together multiple diverse teams operating at different levels with different priorities”

“Intelligence Driven Incident Response” by Scott J. Roberts & Rebekah Brown


SOC Analysts
Threat Hunting Teams
Для
Кого этот
отчёт
Cyber Threat
Intelligence
Analysts
Digital
Forensics
Specialists
Cyber security
specialists who are
involved in the
incident response

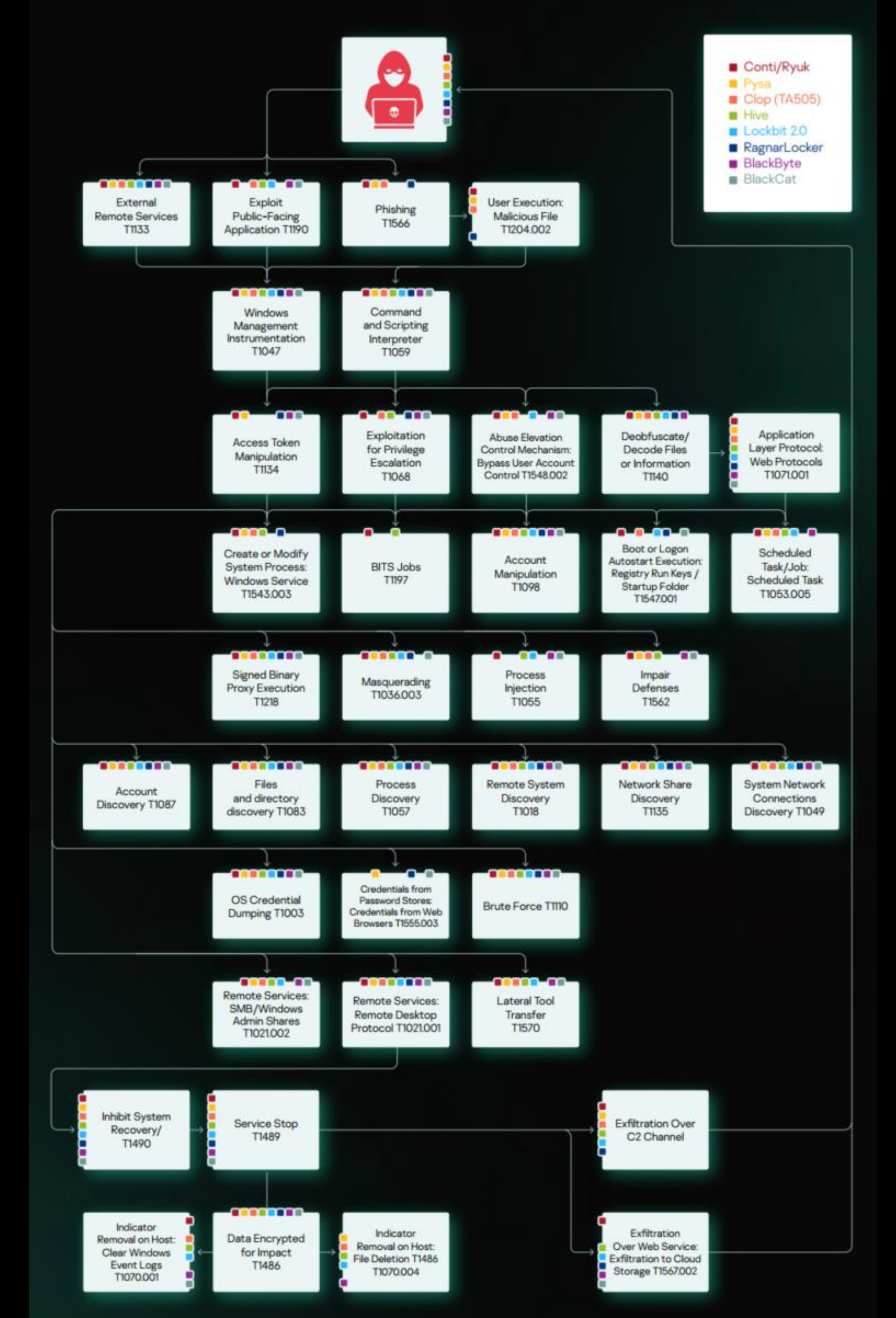

На основе нашей статистики мы составили график появления новых группировок Ransomware:
7
6
5
4
3
2
1
PClock
WannaCry
Erebus
PetWrap
Crypat
Hermes
AecHu
Matrix
Pycl
BTCWare
Poster
Ranion
Tiny
Everbe
Manna
Ferber
Jaff
Rao
Savant
Fairy
MacRansom
Erebus
NotPetya
Nubi
Magni
Pyrgen
BadRabbit
Phobos
Ordin
Clop
GandCrab
WhiteRose
BlackHeart
Ryuk
LimeRat
WannaCash
Scrobo
Dcrtr
Stop/DJVU
Anatova
MegaCortex
Vega
JNEC
RobbinHood
JSWorm
Wesker
Maze
VoidCrypt
DoppelPaymer
NetWalker
Medusa
Snatch
Thanos
NextCry
WastedLocker
Lockbit
PwndLocker
DMR
Makop
Bitpylock
RagnarLocker
Conti
Cuba
Sorena
TeslaRvng
Blackin
WannaRen
Ransomexx
Sfile
Snake
Avaddon
GottaCrypt
EvilQuest
Fonix
Xcrypto
Erica
Darkside
XmrLocker
MountLocker
Egregor
HelloKitty
CoronaLock
Suncrypt
DeathRansom
Cring
Babuk
Hades
Lorenz
Pysa
Quoter
Jesus
Qlocker
DiscoRan
Everest
Hive
Zikma
AvosLocker
Scrypt
BlackMatter
Loki
LockFile
Chaos
Blackbyte
Colossus
Diavol
Prans
Polaris
Rook
Surtr
Sabbath
BlackCat
NightSky
Stormous
Krus
Hermetic
Freeud
Pandora
2017 - Feb
2017 - Mar
2017 - Apr
2017 - May
2017 - Jun
2017 - Aug
2017 - Oct
2017 - Nov
2017 - Dec
2018 - Jan
2018 - Apr
2018 - Aug
2018 - Sep
2018 - Oct
2018 - Nov
2019 - Jan
2019 - Feb
2019 - Mar
2019 - May
2019 - Jun
2019 - Jul
2019 - Sep
2019 - Oct
2019 - Nov
2019 - Dec
2020 - Jan
2020 - Feb
2020 - Mar
2020 - Apr
2020 - May
2020 - Jun
2020 - Jul
2020 - Aug
2020 - Sep
2020 - Oct
2020 - Nov
2020 - Dec
2021 - Jan
2021 - Mar
2021 - Apr
2021 - May
2021 - Jun
2021 - Jul
2021 - Aug
2021 - Sep
2021 - Oct
2021 - Nov
2021 - Dec
2022 - Jan
2022 - Feb
2022 - Mar

Мы выбрали восемь наиболее активных групп Ransomware, а именно:

1. Conti/Ryuk
2. Pysa
3. Clop (TA505)
4. Hive
5. Lockbit2.0
6. RagnarLocker
7. BlackByte
8. BlackCat

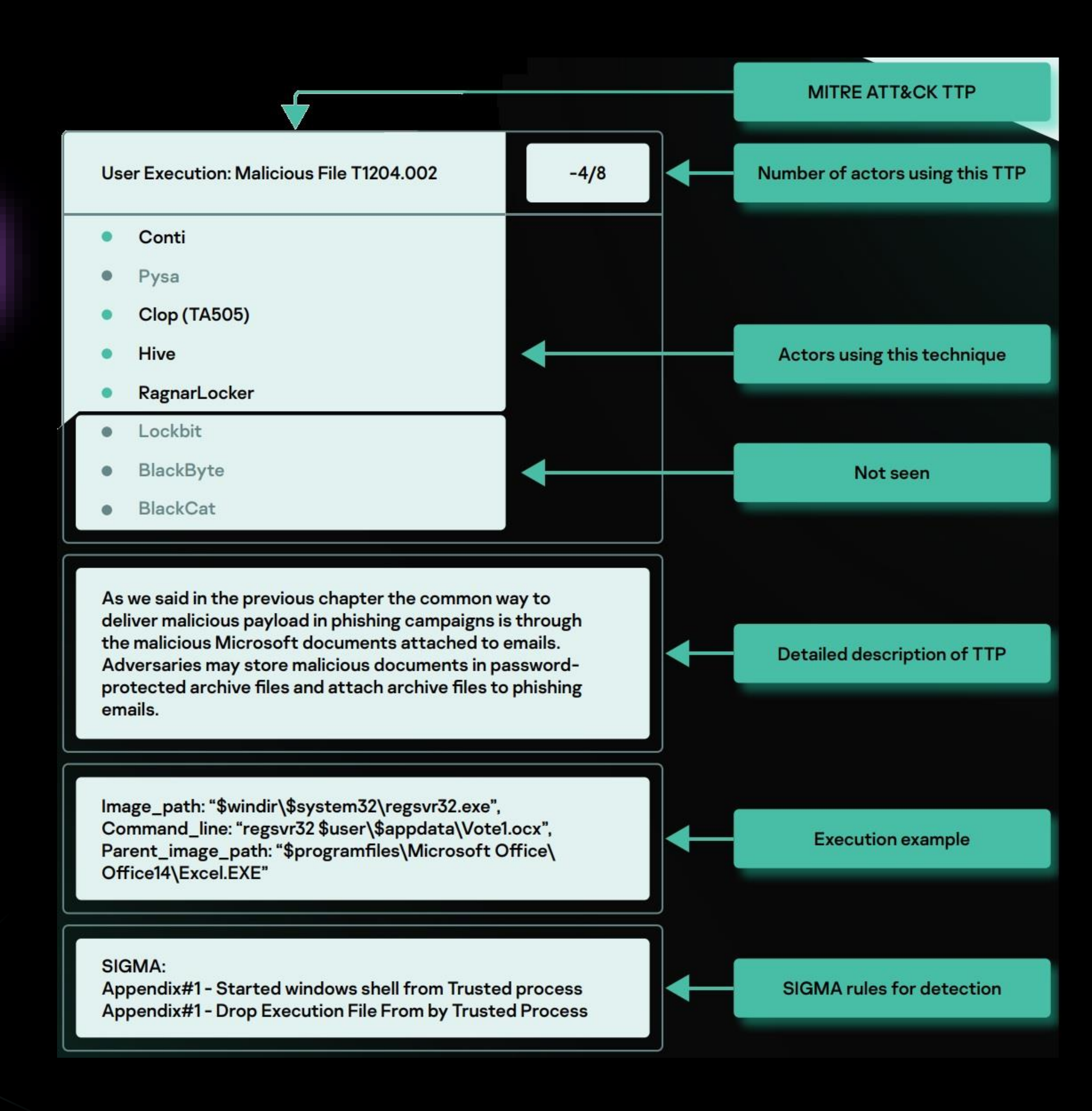
Cyber Kill Chain

Чтобы выделить общие паттерны различных схем атак и TTPs, используемые различными группами вымогателей, мы создали диаграмму Cyber Kill Chain.



Technical Details

Каждая из техник, показанная на предыдущей диаграмме, сопоставлена с группами и сопровождается таблицей, показывающей, кто из обсуждаемых группировок использовал данную технику.



Common TTPs

Tactic								
Initial Access	External Remote Services T1133	Exploit Public Facing Application T1190	Phishing T1566					
Execution	User Execution: Malicious File T1204.002	Command and Scripting Interpreter T1059	Windows Management Instrumentation T1047					
Persistence	Scheduled Task T1053.005	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder T1547.001	Account Manipulation T1098	Create or Modify System Process: Windows Service T1543.003	BITS Jobs T1197			
Privilege Escalation	Abuse Elevation Control Mechanism: Bypass User Account Control T1548.002	Exploitation for Privilege Escalation T1068	Access Token Manipulation T1134					
Defense Evasion	Signed Binary Proxy Execution T1218	Process Injection T1055	Impair Defenses: Disable or Modify System Firewall T1562.004	Impair Defenses: Disable or Modify Tools T1562.001	Masquerading T1036	Indicator Removal on Host: File Deletion T1070.004	Indicator Removal on Host: Clear Windows Event Logs T1070.001	Deobfuscate/ Decode Files or Information T1140
Credential Access	OS Credential Dumping: LSASS Memory T1003.001	Credentials from Password Stores: Credentials from Web Browsers T1555.003	Brute Force T1110					
Discovery	System Network Connections Discovery T1049	Remote System Discovery T1018	Network Share DiscoveryT1135	Account Discovery T1087	File and Directory Discovery T1083	Process Discovery T1057		
Lateral Movement	Remote Services: Remote Desktop Protocol T1021.001	Lateral Tool Transfer T1570	Remote Services: SMB/ Windows Admin Shares T1021.002					
Command and Control	Application Layer Protocol: Web Protocols T1071.001							
Exfiltration	Exfiltration Over C2 Channel T1041	Exfiltration Over Web Service: Exfiltration to Cloud Storage T1567.002						
Impact	Inhibit System Recovery T1490	Service Stop T1489						

Mitigations

Мы собрали лучшие практики из NIST, NCSC, CISA, SANS в организованную структуру, которую можно применять в организациях.

We highlight the following stages of a ransomware incident, that can be mitigated or hampered for adversaries by defenders:

Intrusion

At the intrusion stage, an adversary tries to break into a protected perimeter
Examples: spear phishing emails, bruteforce internet-facing services (RDP)

The Defenders' Main Goal:
Prevent the malware from reaching the devices

Exploitation

At the exploitation stage, an adversary tries to run code in order to escalate privileges, access and exfiltrate sensitive information, or harvest credentials

The Defenders' Main Goal:
Prevent malware from launching on endpoint devices

Lateral Movement

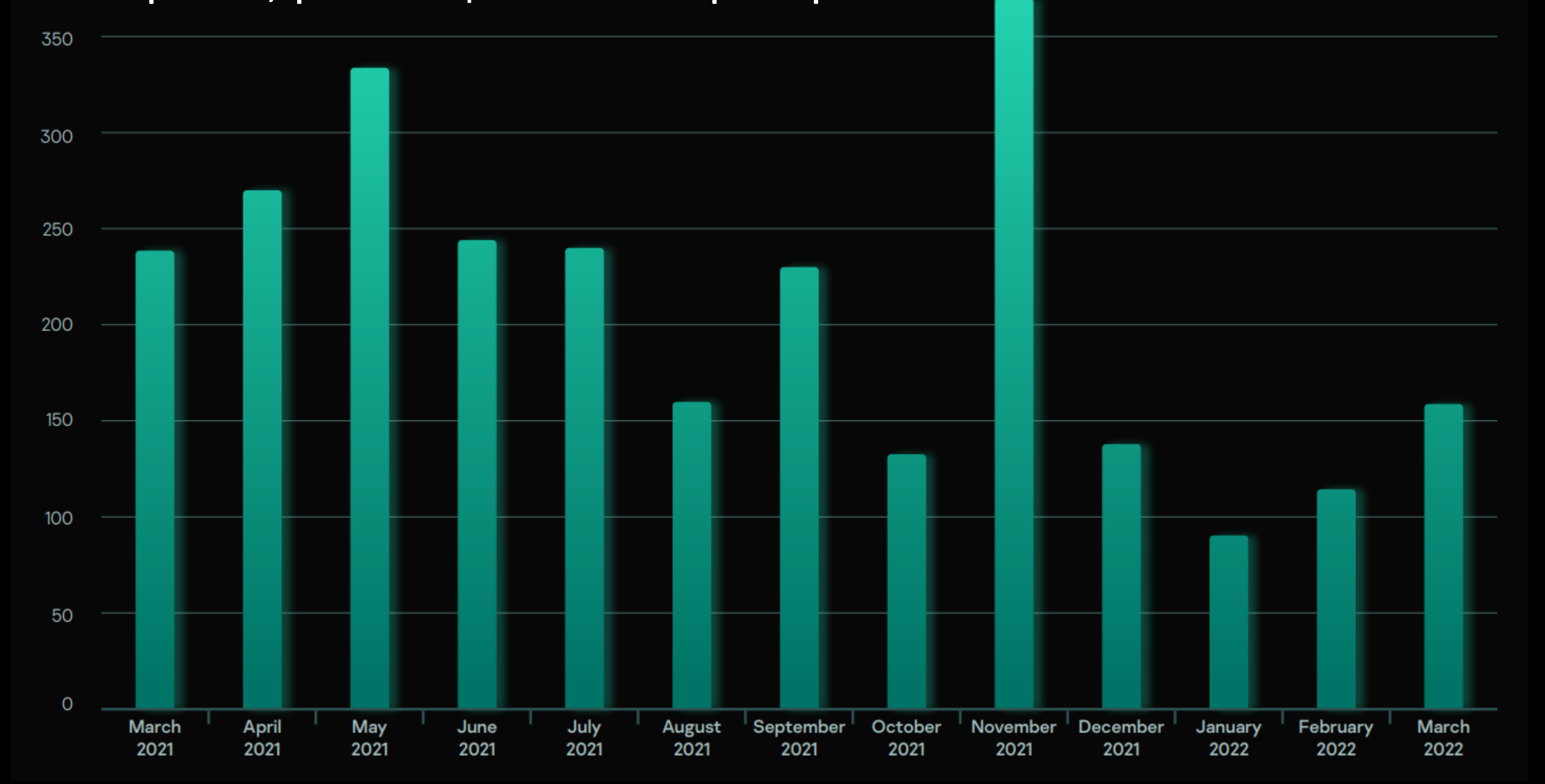
At the lateral movement stage, an adversary tries to spread across the network

The Defenders' Main Goal:
Prevent malware from reaching other devices

There are additional measures that can be taken to make your organization more secure: Countering data loss and Preparing for an incident

Victims

Для этого анализа мы использовали статистические источники по обнаружениям, а также источники объявлений в даркнете о жертвах, размещенных операторами Ransomware.



Sigma Rules

Также мы создали SIGMA правила которые вы можете использовать в своих SIEM системах чтобы обнаруживать активность противника в собственной инфраструктуре.

Techniques	SIGMA
Exploit Public-Facing Application T1190	• Windows Shell Start by Web Applications
User Execution T1204	• Started windows shell from Trusted process • Drop Execution File From by Trusted Process
Command and Scripting Interpreter T1059	Available in the full version of the report in Kaspersky TIP: • Execution of Downloaded Powershell Code • Encoded/decoded PowerShell Code Execution • Executing PS1 from Public Directory • Powershell Suspicious Arguments • Executing JavaScript from Public Directories
Windows Management Instrumentation T1047	Available in the full version of the report in Kaspersky TIP: • Suspicious Command wmic.exe • Suspicious Child Process Wmiprvse.exe
Scheduled Task/Job: Scheduled Task T1053.005	• Scheduled Task Start from Public Directory • Windows Shell Started Schtasks
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder T1547.001	Available in the full version of the report in Kaspersky TIP: • Modification Main Registry Run Keys • Adding Path of Open Folder in Run Keys via Registry • Adding Suspicious File in Autorun Keys via Registry • Suspicious File Creation in Startup Folder
Account Manipulation T1098	Available in the full version of the report in Kaspersky TIP: • Account Creation via Powershell • Account Creation via net.exe • Adding Account in Domain or Local Admin Group via net.exe • Adding Account in Domain or Local Admin Group via PowerShell
Create or Modify System Process: Windows Service T1543.003	Available in the full version of the report in Kaspersky TIP: • Service Installation From Non-System Directory • Service Image Path Modification via sc.exe
BITS Jobs T1197	Available in the full version of the report in Kaspersky TIP: • File Download via Bitsadmin • Suspicious Jobs via Bitsadmin
Abuse Elevation Control Mechanism: Bypass User Account Control T1548.002	• UAC Bypass via COM Object • Disabling UAC via Registry

No More Ransom! Don’t!



“Иногда есть возможность помочь пользователю, зараженному Ransomware, вернуть доступ к зашифрованным данным без уплаты выкупа.

Мы создали коллекцию ключей и утилит, которые могут помочь пользователям восстановить доступ к своим системам, атакованным Ransomware группировками.

Report



Vote



Thank you!

kaspersky